UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/920,740	08/03/2001	Marco Martens	YOR920000722US1	5936

30743 7590 03/23/2007
WHITHAM, CURTIS & CHRISTOFFERSON & COOK, P.C.
11491 SUNSET HILLS ROAD
SUITE 340
RESTON, VA 20190

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	**PAPER NUMBER**
3621	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 09/920,740	**Applicant(s)** MARTENS ET AL.
	Examiner Charlie C. Agwumezie	**Art Unit** 3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 August 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-13, 25-30, and 33-35, are rejected under 35 U.S.C. 102(e) as being anticipated by Davis et al U.S. Patent No. 6,961,849 B1.

As per **claims 1 and 25**, Davis et al discloses a method of protecting a document which will be transformed into a value bearing instrument after adding additional markings to the document from fraudulent alteration of the markings comprising the steps of:

generating encryptions of a unique identifier X of the document, the unique identifier X being printed on the document (fig. 5; col. 18, lines 40-65; ...key strength identifier or encryption algorithm identifier or document identifier...); and

covering each critical field k, k=1,2,3. . . , of the document where markings are to be added with encrypted versions of X, Sign.sub.k,0(X), where Sign.sub.k,0(X) is a cryptographic function or family thereof which is known only to an institution which issues the document, Sign.sub.k,0(X) being used to authenticate the document (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security...provide selective data encryption technique...).

As per **claims 2, 26 and 33**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein an entire area of a field k is covered with a large number of lines of fine print, the lines of fine print comprising one of several encryptions of X (col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per **claims 3, 27, and 34**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein each critical field k of the document, in addition to being covered by the encrypted version of X, Sign.sub.k,0(X), is covered with another encrypted version of X, Sign.sub.k(X), where Sign.sub.k(X) is another cryptographic function or family thereof different from the cryptographic function Sign.sub.k,0(X) which is known to a larger number of authorized institutions for performing an initial authentication of the document (col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per **claim 4**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein each critical field k of the document, in addition to being covered by the encrypted version of X, Sign.sub.k,0(X), is covered with another encrypted version of X, Sec.sub.k(X), where Sec.sub.k(X) is another cryptographic function or family thereof different from the cryptographic function Sign.sub.k,0(X) which is known to a small group within the institution which issues the document for performing final authentication of the document (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security)

As per **claims 5, 28, and 35**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein each critical field k of the document, in addition to being covered by encrypted versions of X, Sign.sub.k(X) and Sign.sub.k,0(X), is covered with a third encrypted version of X, Sec.sub.k(X), where Sec.sub.k(X) is another cryptographic function or family thereof different from the cryptographic functions Sign.sub.k,0(X) and Sign.sub.k(X) which is known to a small group within the institution which issues the document for performing final authentication of the document (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per **claims 6 and 29**, Davis et al further discloses the method of protecting a document from fraudulent alteration, further comprising the step of indexing the cryptographic functions Sign.sub.k, Sign.sub.k,0 and Sec.sub.k, by a number corresponding to the field k, so that each line comprises different encryptions of X such that each cryptographic function Sign.sub.k(X), Sign.sub.k,0(X) and Sec.sub.k(X) is a family of different cryptographic functions (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per **claims 7 and 30**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein the families of cryptographic functions Sign.sub.k, Sign.sub.k,0 and Sec.sub.k prevent cryptographic functions which have been obscured at different places by marks added to the document from being used to reconstitute the full cryptographic function (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per **claim 8**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein electronic deposit of a document transformed into a value bearing instrument comprises the steps of:

scanning the document with a scanner to generate a digitized version of the document (see fig. 7c; col. 26, lines 25-45; col. 27, line 55-col. 28, line 10); and

transmitting the digitized version of the document for deposit (see fig. 7c; col. 1, lines 25-35; col. 26, lines 25-45).

As per **claim 9**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein electronic deposit of a document transformed into a value bearing instrument further comprises the step of endorsing the document, if needed, having printed thereon encryptions in at least selected locations where markings are added to transform the document into a value bearing instrument, the act of endorsing obscuring some of the encryptions (col. 1, lines 25-35; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per **claim 10**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein electronic deposit of a document transformed into a value bearing instrument further comprises the steps of:

extracting from the digitized version of the document the unique identifier X and a corresponding digital encryption of X, Sign.sub.k(X), which is known to a large number of authorized institutions (col. 2, lines 10-40; col. 3, lines 25-35); and comparing a decrypted version of Sign.sub.k(X) to the unique identifier X as an initial authentication of the document (col. 2, lines 50-65).

As per **claim 11**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein electronic deposit of a document transformed into a value bearing instrument further comprises the steps of:

extracting from the digitized version of the document the unique identifier X and a corresponding digital encryption of X, Sign.sub.k,0(X), which is known only to an institution that issues the document (col. 2, lines 10-40; col. 3, lines 25-35); and

comparing a decrypted version of Sign.sub.k,0(X) to the unique identifier X as a further authentication of the document (col. 2, lines 50-65).

As per **claim 12**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein electronic deposit of a document transformed into a value bearing instrument further comprises the steps of:

extracting from the digitized version of the document the unique identifier X and a corresponding digital encryption of X, Sec.sub.k(X), which is known to a small group within the institution that issues the document (col. 2, lines 10-40; col. 3, lines 25-35); and

comparing a decrypted version of Sec.sub.k(X) to the unique identifier X as a final authentication of the document (col. 2, lines 50-65).

As per **claim 13**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein portions of the lines of fine print are obscured by writing added to the document when transforming the document into a value bearing instrument (col. 1, lines 25-35).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 14-17, 18, 19-24, 31-32, and 36-38, are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al U.S. Patent No. 6,961,849 B1 in view of Buchanan et al U.S. Patent No. 7,181,430 B1.

As per **claims 14 and 31**, Davis et al failed to explicitly disclose the method of protecting a document from fraudulent alteration, wherein the document is a check and the unique identifier X is check data comprising a bank Id number, an account Id number and a check number.

Buchanan et al discloses the method of protecting a document from fraudulent alteration, wherein the document is a check and the unique identifier X is check data comprising a bank Id number, an account Id number and a check number (col. 8, lines 25-45; col. 11, lines 45-60).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a document from fraudulent alteration, wherein the document is a check and the unique identifier X is check data comprising a bank Id number, an account Id number and a check number in view of the teachings of Buchanan et al in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

15. As per **claim 15**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein an issuing bank chooses a first secret key Sign.sub.k using a secure cryptographic generator (SCG), further comprising the steps of:

computing a first family of encrypted functions Sign.sub.k(X) (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security); and

communicating the key Sign.sub.k to banks and other authorized institutions involved in depositing of checks, the family of encrypted functions Sign.sub.k(X) allowing the payee's bank to perform a first authentication of the check (see fig. 7c; col. 1, lines 25-35; col. 26, lines 25-45).

What Davis does not explicitly teach is that the document is check and process involved in depositing of checks.

Buchanan et al discloses that the document is check and the process involved in depositing the check (see figs. 5 and 7)

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a document from fraudulent alteration, wherein the document is a check and the process involved in depositing the check in view of the teachings of Buchanan et al in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

16. As per **claim 16**, Davis et al discloses the method of protecting a document from fraudulent alteration, wherein an issuing bank chooses a second secret key Sign.sub.k,0 using a SCG, further comprising the steps of:

computing a second family of encrypted functions Sign.sub.k,0(X), key Sign.sub.k,0 remaining the exclusive property of the issuing bank (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security); and

using SCGs, communicating the key Sign.sub.k,0 to all branches of the issuing bank where check clearing is done, the family of encrypted functions Sign.sub.k,0(X) being used exclusively by the issuing bank and branches involved in the clearing of checks (see fig. 4; col. 1, lines 25-35; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

17. As per **claim 17**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein an issuing bank chooses a third secret key Sec.sub.k which is exclusively known to a small group within the issuing bank, further comprising the step of computing a third family of encrypted functions Sec.sub.k(X), the secret key Sec.sub.k being used by the issuing bank as final instrument to verify the check (see fig. 4; col. 1, lines 25-35; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

18. As per **claim 18**, Davis et al failed to explicitly disclose the method of protecting a document from fraudulent alteration, wherein the check is deposited by a payee electronically from a location remote from a bank or Automatic Teller Machine (ATM).

Buchanan et al discloses the method of protecting a document from fraudulent alteration, wherein the check is deposited by a payee electronically from a location remote from a bank or Automatic Teller Machine (ATM) (col. 1, lines 35-45; col. 2, lines 10-35).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a document from fraudulent alteration, wherein the check is deposited by a payee electronically from a location remote from a bank or Automatic Teller Machine (ATM) in view of the teachings of Buchanan et al in order to encourage the convenience of depositing check data from remote locations distinct from bank or ATM.

19. As per **claim 19**, Davis et al failed to explicitly disclose the method of protecting a document from fraudulent alteration, wherein electronic deposit of the check by a payee comprises the steps of:

endorsing the check having printed thereon encryptions in at least selected locations where information is written by a payer, the act of endorsing by the payee obscuring some of the encryptions; scanning the endorsed check with a scanner to generate a digitized version of the check; transmitting the digitized version of the check for deposit to the payee's bank. Davis however discloses that the system is useful for data that is to be securely stored, such as the account records for customers of a bank or credit company.

Buchanan et al discloses endorsing the check having printed thereon encryptions in at least selected locations where information is written by a payer, the act of endorsing by the payee obscuring some of the encryptions (see figs. 5 and 7; col. 2, lines 10-50);

scanning the endorsed check with a scanner to generate a digitized version of the check (see figs. 5 and 7); transmitting the digitized version of the check for deposit to the payee's bank (see figs. 5 and 7).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a document from fraudulent alteration, wherein endorsing the check having printed thereon encryptions in at least selected locations where information is written by a payer, the act of endorsing by the payee obscuring some of the encryptions; scanning the endorsed check with a scanner to generate a digitized version of the check; transmitting the digitized version of the check for deposit to the payee's bank in view of the teachings of Buchanan et al in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

20. As per **claim 20**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein electronic deposit of the check by a payee comprises the steps of:

extracting by the payee's bank from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, Sign.sub.k(X), which is known to a large number of authorized institutions including the payee's bank (col. 2, lines 10-40; col. 3, lines 25-35); and

comparing by the payee's bank a decrypted version of Sign.sub.k(X) to the unique identifier X as an initial authentication of the check (col. 2, lines 50-65).

What Davis does not explicitly teach is that the document is a check. Davis however discloses that the system is useful for data that is to be securely stored, such as the account records for customers of a bank or credit company.

Buchanan discloses that the document is a check (see figs. 1, 5, and 7).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a document from fraudulent alteration, wherein the document is a check in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

21. As per **claim 21**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein electronic deposit of the check further comprises the steps of:

extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, Sign.sub.k,0(X), which is known only to a bank that issues the check (col. 2, lines 10-40; col. 3, lines 25-35); and

comparing by the payor's bank a decrypted version of Sign.sub.k,0(X) to the unique identifier X as a further authentication of the check (col. 2, lines 50-65).

What Davis does not explicitly teach is that the document is a check. Davis however discloses that the system is useful for data that is to be securely stored, such as the account records for customers of a bank or credit company.

Buchanan discloses that the document is a check (see figs. 1, 5, and 7).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a document from fraudulent alteration, wherein the document is a check in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

22. As per **claim 22**, Davis et al further discloses the method of protecting a document from fraudulent alteration, wherein electronic deposit of the check further comprises the steps of:

extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, Sec.sub.k(X), which is known to a small group within the bank that issues the check (col. 2, lines 10-40; col. 3, lines 25-35); and

comparing a decrypted version of Sec.sub.k(X) to the unique identifier X as a final authentication of the check (col. 2, lines 50-65).

What Davis does not explicitly teach is that the document is a check. Davis however discloses that the system is useful for data that is to be securely stored, such as the account records for customers of a bank or credit company.

Buchanan discloses that the document is a check (see figs. 1, 5, and 7).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a document from fraudulent alteration, wherein the document is a check in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

23. As per **claim 23**, Davis et al failed to explicitly disclose the method of protecting a document from fraudulent alteration, further comprising the step of accessing a database by the payee's bank where the unique identifier X and first encrypted function Sign.sub.k(X) is registered to determine whether the check has been previously presented for deposit.

Buchanan et al discloses the method of protecting a document from fraudulent alteration, further comprising the step of accessing a database by the payee's bank where the unique identifier X and first encrypted function Sign.sub.k(X) is registered to determine whether the check has been previously presented for deposit (col. 13, line 45-col. 14, line 5; col. 17, lines 10-55; ...determines whether item is payable or not...).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a document from fraudulent alteration, further comprising the step of accessing a database by the payee's bank where the unique identifier X and first encrypted function Sign.sub.k(X) is registered to determine whether the check has been previously presented for deposit in order to prevent fraud of deposit one same check multiple times.

24. As per **claim 24**, Davis et al failed to explicitly disclose the method of protecting a

document from fraudulent alteration, further comprising the step of registering a check to be deposited by the payee with an SCG to prevent multiple deposits.

Buchanan et al discloses the method of protecting a document from fraudulent alteration, further comprising the step of registering a check to be deposited by the payee with an SCG to prevent multiple deposits (col. 13, line 45-col. 14, line 5; col. 17, lines 10-55; ...determines whether item is payable or not...).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method method of protecting a document from fraudulent alteration, further comprising the step of registering a check to be deposited by the payee with an SCG to prevent multiple deposits in order to avoid multiple deposit one same check through the remote deposit of checks.

32. As per **claim 32**, Davis et al further discloses the document, wherein the act of adding markings to the check to transform the document into a value bearing instrument obscures some of the encryptions (fig. 4)

36. As per **claim 36**, Davis et al failed to explicitly disclose the document, wherein the encrypted function Sign.sub.k(X) are communicated to banks and other authorized institutions involved in depositing checks and the encrypted function Sign.sub.k(X) allows the payee's bank to perform a first authentication of the check. Davis however

discloses that the system is useful for data that is to be securely stored, such as the account records for customers of a bank or credit company.

Buchanan et al discloses the document, wherein the encrypted function Sign.sub.k(X) are communicated to banks and other authorized institutions involved in depositing checks and the encrypted function Sign.sub.k(X) allows the payee's bank to perform a first authentication of the check (see figs. 5 and 7; col. 9, line 40-col. 10 , line 5).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method wherein the encrypted function Sign.sub.k(X) are communicated to banks and other authorized institutions involved in depositing checks and the encrypted function Sign.sub.k(X) allows the payee's bank to perform a first authentication of the check in view of the teachings of Buchanan et al in order to prevent fraud and ensure adequate security of remote deposit of checks.

37. As per **claim 37**, Davis et al further discloses the document, wherein key Sign.sub.k,0 remains the exclusive property of the issuing bank and the encrypted function Sign.sub.k,0(X) is used exclusively by the issuing bank and branches involved in the clearing of checks (col. 3, lines 25-35; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

38. As per **claim 38**, Davis et al further discloses the document, wherein secret key Sec.sub.k is exclusively known to the issuing bank and the encrypted function Sec.sub.k(X) is used by the issuing bank as a final instrument to verify the check (col. 3, lines 25-35).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The references cited to Rucklidge et al U.S. Patent No. 6,449,718 and Kluttz et al U.S. Patent No. 6,598,161 B1 are documents considered relevant to the claimed invention.

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art ad are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on **(571) 272 – 6779**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Charlie Lion Agwumezie
Patent Examiner
Art Unit 3621

Acc
March 10, 2007

AJ Fischer 3/19/07

ANDREW J. FISCHER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600